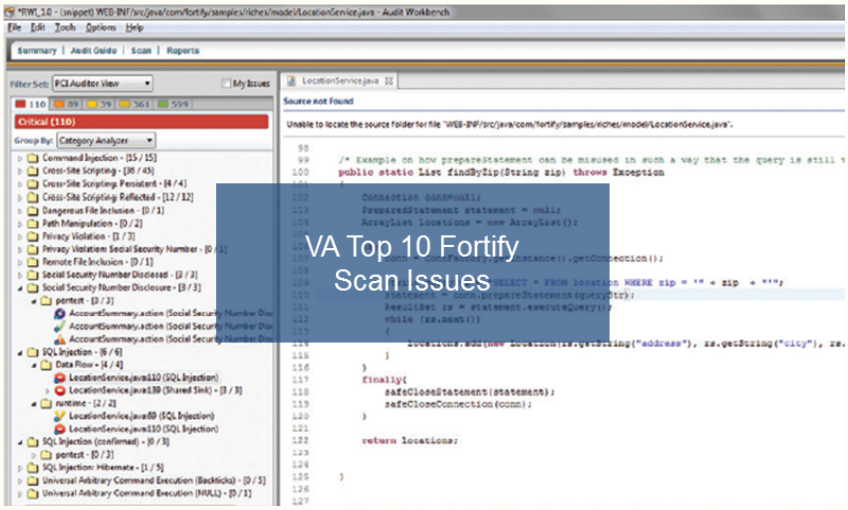
VA Top 10 Fortify Scan Issues

Register your application, request VA-licensed Fortify software, training, and support HERE

This page has been made public for vendors



VA Top 10 Fortify Scan Issues

The VA Software Assurance Program Office is pleased to announce the release of its list of the most common issues encountered at the VA when scanning source code using the HPE Fortify Static Code Analyzer (SCA) tool, according to the **VA Secure Code Review Standard Operating Procedures (SOP)**.

The **VA Secure Code Review SOP** is the means by which Office of Information and Technology (OI&T) implements standard repeatable processes for performing Static Application Security Testing (SAST) during VA application development across the organization.

Code review is included in the Technical / Testing Requirements as part of the **Office of Cyber Security (OCS) Accreditation Requirements Guide / SOP [1]** and **VA Secure Code Review SOP**, and enforced as part of the Authority to Operate (ATO) issuance process.**[2]**

This list does not contain any vulnerability information. This list can be used to learn from the mistakes of others. And, to help System Owners, Project Managers, Information Security Officers (ISOs), and all system / project / contractor staff with furthering awareness of the risk that software creates at the VA.

The **VA Top 10 Fortify Scan Issues For 2017 (Q2)** are:

- **S1:** Code not scanned
- **S2:** Errors during scan
- **S3:** Scanned source differs from provided source
- **S4:** Code scanned but not delivered
- **S5:** Old version of Fortify used during scan
- **S6:** Old version of rulepacks used during scan
- **S7**: Hidden and suppressed issues
- **S8:** Issues not audited
- **S9:** Buildable source not delivered
- **S10:** Default rulepacks were not used during scan

This list is the result of actual code review validations performed according to the **VA Secure Code Review SOP** by the VA Software Assurance Program Office.

---

[1] Reference: “Accreditation Requirements Guide / Standard Operating

VA Common Scan Issues Archives:

- **2017 (Q1)**
- **2016 (Q4)**
- **2016 (Q3)**
- **2016 (Q2)**
- **2016 (Q1)**
- **2015 (Q4)**
- **2015 (Q3)**
- **2015 (Q2)**
- **2015 (Q1)**

Procedures", OCS Assessment and Authorization intranet site.

[2] Reference: "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.